Available online at www.sciencedirect.com

ScienceDirect

Discrete Applied Mathematics 156 (2008) 76–81

DISCRETE APPLIED MATHEMATICS

www.elsevier.com/locate/dam

Note

Cyclically permutable representations of cyclic codes

Derek H. Smith*, Stephanie Perkins

Division of Mathematics and Statistics, University of Glamorgan, Pontypridd, CF37 1DL Wales, UK

Received 29 March 2006; received in revised form 28 June 2007; accepted 12 August 2007
Available online 29 September 2007

Abstract

Cyclically permutable codes have been studied for several applications involving synchronization, code-division multiple-access (CDMA) radio systems and optical CDMA. The usual emphasis is on finding constant weight cyclically permutable codes with the maximum number of codewords. In this paper the question of when a particular error-correcting code is equivalent (by permutation of the symbols) to a cyclically permutable code is addressed. The problem is introduced for simplex codes and a motivating example is given. In the final section it is shown that the construction technique may be applied in general to cyclic codes.

Keywords: Cyclic codes; Cyclically permutable codes; Simplex codes

1. Introduction

A *cyclically permutable code* is a binary block code of length n such that each codeword has n distinct cyclic shifts and such that no codeword can be obtained by one or more cyclic shifts of another codeword. Cyclically permutable codes were introduced in [2] and have been further studied in several papers, including [6,7,1,5]. Applications can be found in, for example, [2,10].

Consider the set of codewords of a given cyclic error-correcting code, excluding the zero codeword and the all 1's codeword if it exists. In this paper the question of when this set is equivalent to a cyclically permutable code (by permutation of the positions of the original cyclic code) is considered. When the equivalence exists the code will be said to have a *cyclically permutable representation*. Some codes clearly have no cyclically permutable representation. Consider Hamming codes of length $n = 2^m - 1$, for example. They have $n(n-1)/6$ codewords of weight 3 and in a cyclically permutable representation the n distinct cyclic shifts of these are all distinct vectors. However, there are only $n(n-1)(n-2)/6$ vectors of weight 3 in total. For other codes it may be possible to find a cyclically permutable representation by a random search algorithm. However, it is important to have a deterministic construction and to be able to determine for which sets of parameters a code will have a cyclically permutable representation. For ease of presentation the construction is illustrated initially for simplex codes (for which a complete answer is given) and is generalized to other cyclic codes in Section 4. An application in the simplex case is given in Section 3.

* Corresponding author.
E-mail addresses: dhsmith@glam.ac.uk (D.H. Smith), sperkins@glam.ac.uk (S. Perkins).

0166-218X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2007.08.038

2. Simplex codes

A simplex code is the dual of a Hamming code [4]. Examples of simplex codes are the cyclic maximum-length-sequence codes [8]. A maximum-length-sequence code is generated by a primitive polynomial of degree m. This polynomial can be considered as the parity check polynomial of a cyclic code of length $n = 2^m - 1$. The fact that the polynomial is primitive ensures that the set of non-zero codewords forms a cyclic sequence of period $2^m - 1$ [8].

Let $\mathbf{x} = (x_0, x_1, \ldots, x_{2^m-2}) \neq \mathbf{0}$ ($m \geqslant 9$) be a single phase of a maximal length sequence generated by a primitive binary polynomial $p(x) = p_0 + p_1x + p_2x^2 + \cdots + p_mx^m$. Thus, the sequence is generated by the binary recurrence relation $p_m x_j = p_{m-1}x_{j-1} + p_{m-2}x_{j-2} + \cdots + p_0x_{j-m}$ ($m \leqslant j \leqslant 2^m - 2$) with $x_0, x_1, \ldots, x_{m-1}$ not all equal to 0. Without loss of generality the phase of the sequence can be chosen so that $x_{2m+1} = 1$. Let the operator $S_j(\mathbf{v})$ denote a cyclic shift of a vector $\mathbf{v}$ by j positions and let the $(2^m - 1) \times (2^m - 1)$ matrix A have rows $\{\mathbf{c}_0 = \mathbf{x}, \mathbf{c}_1 = S_1(\mathbf{c}_0), \mathbf{c}_2 = S_2(\mathbf{c}_0), \ldots, \mathbf{c}_{2^m-2} = S_{2^m-2}(\mathbf{c}_0)\}$. The rows $\mathbf{c}_i$ of A are the non-zero codewords of a cyclic simplex code.

Lemma 1. *No m consecutive entries of any codeword $\mathbf{c}_i$ can all be* 0.

Proof. If they were the sequence generated would not be a maximal length sequence but the zero sequence. □

Lemma 2. *No $m + 1$ consecutive entries of any codeword $\mathbf{c}_i$ can all be* 1.

Proof. If they were the recurrence relation (or shift register) generating the sequence would always follow m 1's with a 1. Thus every subsequent element of the sequence is a 1. The sequence generated would not be a maximal length sequence but the all 1's sequence. □

Lemma 3. *The Hamming distance between any pair of codewords of a simplex code is 2^{m-1}* [4].

Lemma 4. *Let A be the matrix defined above. Assume without loss of generality that the first codeword has a* 1 *in position $i_1 = 2m + 1$. Then for a sufficiently long code it is possible to define a set of positions $i_1, i_2, \ldots, i_{m+1}$ so that*

(1) $i_1 \leqslant i_2 \leqslant \cdots \leqslant i_{m+1}$,
(2) $m + 1 \leqslant i_{j+1} - i_j \leqslant 2m$ *for* $1 \leqslant j \leqslant m - 1$,
(3) $m + 1 \leqslant i_{j+1} - i_j \leqslant 2m + 1$ *for* $j = m$

in such a way that no row of A is zero in all of these positions and no row of A is 1 *in all of these positions.*

Proof. Add row 1 of A to all other rows with a 1 in position $i_1 = 2m + 1$ and remove duplicate rows. Now find the first position i_2 with $m + 1 + i_1 \leqslant i_2 \leqslant 2m + i_1$ such that the second row has a 1 in this position (a choice guaranteed by Lemma 1). Add the second row to all other rows with a 1 in position i_2 and remove all duplicate rows. Continue this process until a generator matrix of m rows is obtained. The submatrix of the generator matrix formed by columns $i_1, i_2, \ldots, i_m$ is a unit matrix I_m. Thus, only one vector of the code has a 0 in the positions $i_1, i_2, \ldots, i_m$ (the zero vector) and this is excluded from A. Similarly, only one vector of the code has a 1 in these positions. Now choose the first position i_{m+1} with $m + 1 + i_m \leqslant i_{m+1} \leqslant 2m + 1 + i_m$ such that this vector has a 0 in position i_{m+1} (a choice guaranteed by Lemma 2). Thus no vector of the code has a 1 in the positions $i_1, i_2, \ldots, i_{m+1}$. □

Proposition 1. *If $m \geqslant 9$ a set of positions $i_1, i_2, \ldots, i_{m+1}$ can be chosen so that*

(1) $i_1 = 2m + 1$ *and* $x_{i_1} = 1$,
(2) $i_1 \leqslant i_2 \leqslant \cdots \leqslant i_{m+1}$,
(3) $m + 1 \leqslant i_{j+1} - i_j \leqslant 2m$ *for* $1 \leqslant j \leqslant m - 1$,
(4) $m + 1 \leqslant i_{j+1} - i_j \leqslant 2m + 1$ *for* $j = m$,
(5) $i_{m+1} \leqslant 2^{m-1} - 1$

in such a way that no row of A is zero in all of these positions and no row of A is 1 *in all of these positions.*

Proof. The phase of the maximal length sequence has been chosen so that $x_{2m+1} = 1$, so (1) holds. Provided property (5) holds the code is long enough and properties (2)–(4) follow from Lemma 4. As $(2m + 2) + (m - 1)2m + (2m + 1) = 2m^2 + 2m + 3 \leqslant 2^{m-1} - 1$ for $m \geqslant 9$ it follows that $i_{m+1} \leqslant 2^{m-1} - 1$, i.e. property (5) holds. □

In the following, the set of positions $i_1, i_2, \ldots, i_{m+1}$ will be referred to as the *comb* and the set of positions $0, 1, \ldots, m$ will be referred to as the *block*. Define an operation P on the matrix A:

Definition 1. Operation P_1 is a single cyclic shift of the columns $0, 1, \ldots, m$ of A (i.e. of the block). Operation P_2 is a single cyclic shift of the columns $i_1, i_2, \ldots, i_{m+1}$ of A (i.e. of the comb). Operation P is defined as operation P_1 followed by operation P_2.

In view of Lemmas 1 and 2 and Proposition 1 each codeword is changed in the positions relevant to the operation P_1 (respectively, P_2) in an even number of positions between 2 and $m + 1$. The following lemma is then immediate.

Lemma 5. *For any codeword* $\mathbf{v}$, *the vectors* $S_j(P(\mathbf{v}))$ *and* $P(S_j(\mathbf{v}))$ *coincide except in a maximum of* $4m+4$ *positions. In consequence, if* $\mathbf{w}$ *is any other codeword then*

$$d(S_j(P(\mathbf{v})),\ P(\mathbf{w})) \geqslant d(P(S_j(\mathbf{v})),\ P(\mathbf{w})) - 4(m + 1) = d(S_j(\mathbf{v}), \mathbf{w}) - 4(m + 1).$$

After an application of operation P to A precisely once, the rows of the matrix (together with a zero codeword) give a simplex code equivalent to the maximal length sequence code. It will now be shown that the non-zero codewords form a cyclically permutable code.

Proposition 2. *Let* A *be the matrix corresponding to a maximal length sequence code with* $m \geqslant 9$. *If the operation* P *is applied to* A *precisely once to give a new matrix* $\tilde{A}$, *then the rows of* $\tilde{A}$ *form a cyclically permutable code.*

Proof. For a maximal length sequence the Hamming distance between a row $S_i(\mathbf{c}_0)$ of A and $S_j(S_i(\mathbf{c}_0))$ ($j \not\equiv 0 \bmod 2^m - 1$) is 2^{m-1} (Lemma 3). It follows from Lemma 5 that the Hamming distance between $P(S_i(\mathbf{c}_0))$ and $S_j(P(S_k(\mathbf{c}_0)))$ is at least $2^{m-1} - 4(m + 1)$ ($i \not\equiv j + k \bmod 2^m - 1$) which is greater than 0 for $m \geqslant 9$. Thus it is only necessary to consider $i \equiv j + k \bmod 2^m - 1$. Consider first the case when $|i - k| \leqslant m$. Then the cyclically shifted combs of the two codewords $P(S_i(\mathbf{c}_0))$ and $S_j(P(S_k(\mathbf{c}_0)))$ are disjoint and are disjoint from the cyclically shifted blocks of both codewords. Thus, the two codewords differ in both combs and the minimum Hamming distance is at least 4. Finally, consider the case when $|i - k| \geqslant m + 1$. Then the cyclically shifted block of one codeword is disjoint from the cyclically shifted block and from the cyclically shifted comb of the other codeword. Thus, the two codewords differ in at least one block and the minimum Hamming distance is at least 2. (This can be improved to 4 by noting that the other block can only overlap with a comb in one position, so the two codewords also differ in the other block in at least one position. However, the Hamming distance must be even.) It follows that each codeword is distinct from a cyclic shift of itself or of any other codeword. Thus the simplex code is cyclically permutable. □

Next we describe a very simple heuristic algorithm to deal with the cases $4 \leqslant m \leqslant 8$.

Algorithm 1. *Let* G *be the generator matrix of an initial simplex code. Randomly choose a pair of columns of* G. *If interchanging these columns would increase the number of cyclically distinct codewords, the interchange is performed. Such interchanges are performed until the number of cyclically distinct codewords is* $2^m - 1$ *or this number ceases to increase.*

As it is easier to remove a cyclic structure than to create one, the algorithm terminates quickly given an arbitrary initial ordering. For example, if $m = 4, 5, 6, 7, 8$ then just 2 or 3 iterations were required.

Theorem 1. *A simplex code has a cyclically permutable representation if and only if* $m \geqslant 4$.

Proof. If $m = 2$ there is at most one cyclically distinct codeword of weight 2. If $m = 3$ there are at most five cyclically distinct codewords of weight 4. Hence cyclically permutable simplex codes with $m = 2$ or 3 cannot

exist. If $4 \leqslant m \leqslant 8$ a cyclically permutable code is obtained by Algorithm 1. If $m \geqslant 9$ the result follows from Proposition 2. □

3. An application

Lin and Chang [3] are concerned with the construction of sets of codewords of length N for which for any pair $\mathbf{X}$,$\mathbf{Y}$ of codewords the cross-correlation

$$\Theta_{\mathbf{X},\mathbf{Y}}(\tau) = \sum_{j=0}^{N-1} (-1)^{X_j + Y_{j+\tau \bmod N}}$$

is small when τ is close to 0. Such codewords are used in code-division multiple-access (CDMA) applications. The autocorrelation $\Theta_{\mathbf{X},\mathbf{X}}(\tau)$ must also be small in the same interval except when $\tau = 0$. Lin and Chang also note that it is preferable to use cyclically distinct codewords.

Let m, n be two integers with m a divisor of n and let $T = (2^n - 1)/(2^m - 1)$. Let α be a primitive element of the finite field $GF(2^n)$ and let $\mathrm{Tr}_m^n(x) = \sum_{j=0}^{n/m-1} x^{2^{mj}}$ be the trace function from $GF(2^n)$ to $GF(2^m)$. Properties of the trace function can be found in [4].

The trace function is used to define a *shift sequence* $S = (s_0, s_1, \ldots, s_{2^n-2})$. Specifically, for $k = 0, 1, 2, \ldots, 2^n - 2$ define s_k by

$$s_k = \begin{cases} i & \text{if } \mathrm{Tr}_m^n(\alpha^k) = \alpha^{Ti}, \quad i \in \{0, 1, \ldots, 2^m - 2\}, \\ \infty & \text{if } \mathrm{Tr}_m^n(\alpha^k) = 0. \end{cases}$$

The sequence $\mathbf{X_e}$ (of length $N = 2^n - 1$), corresponding to a *seed vector* $\mathbf{e} = (e_0, e_1, \ldots, e_{2^m-2})$, is then constructed from a $(2^m - 1) \times T$ array with columns labelled $0, 1, \ldots, T - 1$ as follows. If s_i is ∞ then the ith column of the array is a column of zeros. If $s_i \neq \infty$ then the ith column is the transpose of $(e_{s_i}, e_{s_{i+1}}, \ldots, e_{s_i + 2^m - 2 \bmod (2^m-1)})$ and thus is a cyclic shift of $\mathbf{e}$. The array is as shown in Fig. 1, with the convention $e_\infty = 0$. Then $\mathbf{X_e}$ is obtained by scanning the rows of this array, starting from the top left-hand corner. Lin and Chang show that the sequence can be written as

$$\mathbf{X_e} = (e_{s_0}, e_{s_1}, \ldots, e_{s_{T-1}}, e_{sT}, \ldots, e_{s_{2(T-1)}}, e_{s_{2T}}, \ldots, e_{s_{2^n-2}}).$$

In a similar way, given a second seed vector $\mathbf{f}$ a sequence can be constructed:

$$\mathbf{X_f} = (f_{s_0}, f_{s_1}, \ldots, f_{s_{T-1}}, f_{sT}, \ldots, f_{s_{2(T-1)}}, f_{s_{2T}}, \ldots, f_{s_{2^n-2}}).$$

Let $\theta_{\mathbf{e},\mathbf{f}}(\tau)$ be the cross-correlation function of the seed vectors.

Theorem 2 (*Lin and Chang [3]*). *If the vectors* $\mathbf{e}$ *and* $\mathbf{f}$ *are balanced vectors* (*i.e. each with* 2^{m-1} 1's), *then*

$$\Theta_{\mathbf{X_e},\mathbf{X_f}}(\tau) = \begin{cases} -1 & \text{for } \tau \not\equiv 0 \,(\mathrm{mod}\, T), \\ 2^{n-m} - 1 + 2^{n-m}\theta_{\mathbf{e},\mathbf{f}}(d) & \text{for } \tau = dT. \end{cases}$$

The same result holds for autocorrelation $\Theta_{\mathbf{X_e},\mathbf{X_e}}(\tau)$ *except when* $\tau = 0$, *when the autocorrelation is* $2^n - 1$.

$$\begin{bmatrix} e_{s_0} & e_{s_1} & \cdots & e_{s_{T-1}} \\ e_{s_0+1} & e_{s_1+1} & \cdots & e_{s_{T-1}+1} \\ \cdot & \cdot & \cdots & \cdot \\ e_{s_0+2^m-2 \bmod (2^m-1)} & e_{s_1+2^m-2 \bmod (2^m-1)} & \cdots & e_{s_{T-1}+2^m-2 \bmod (2^m-1)} \end{bmatrix}$$

Fig. 1. The $(2^m - 1) \times T$ array used to construct the sequence $\mathbf{X_e}$.

Lin and Chang propose the use of the set of all balanced sequences for the seed vectors, but the correlation may not be small when $\tau = 0$. It is well known that the choice of all different phases of an m-sequence for $\mathbf{e}$ gives different equally spaced phases of a single m-sequence for $\mathbf{X}_\mathbf{e}$. However, it was noted recently [9] that if the seed vectors are the (non-zero) codewords of a cyclically permutable representation of a simplex code then $2^m - 1$ cyclically distinct codewords of full period are obtained with $\Theta_{\mathbf{X}_\mathbf{e},\mathbf{X}_\mathbf{f}}(\tau) = -1$ for $|\tau| < T$ as required. The fact that the codewords are cyclically distinct allows conventional synchronization techniques to be used, and allows for timing error.

4. Starting from other cyclic codes

In this section it will be shown that the proof technique of Section 2 can be applied to certain cyclic codes. The primitive binary polynomial for maximal length sequences is replaced by the parity check polynomial [8] of degree m of the chosen cyclic code of length n. It is also sometimes necessary to exclude the all ones vector as well as the zero vector in the cyclically permutable code. The initial cyclic code must have large minimum distance.

Let Ω denote the number of distinct cyclic sets in the linear code, excluding the zero vector and the all ones vector if the code contains it. Denote the number of vectors in the cyclic sets by $\lambda_0, \lambda_1, \ldots, \lambda_{\Omega-1}$. Let $\mathbf{x}^{(0)}, \mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(\Omega-1)}$ be representatives of these cyclic sets. For the general cyclic case the matrix A must be modified. It will have rows

$$\{\mathbf{x}^{(0)}, S_1(\mathbf{x}^{(0)}), S_2(\mathbf{x}^{(0)}), \ldots, S_{(\lambda_0-1)}(\mathbf{x}^{(0)}), \mathbf{x}^{(1)}, S_1(\mathbf{x}^{(1)}), S_2(\mathbf{x}^{(1)}), \ldots,$$
$$S_{(\lambda_1-1)}(\mathbf{x}^{(1)}), \ldots, \mathbf{x}^{(\Omega-1)}, S_1(\mathbf{x}^{(\Omega-1)}), S_2(\mathbf{x}^{(\Omega-1)}), \ldots, S_{(\lambda_{\Omega-1}-1)}(\mathbf{x}^{(\Omega-1)})\}.$$

Lemma 6. *No m consecutive entries of any row of A can all be* 0.

Proof. If they were the cyclic set of codewords generated by the parity check polynomial would consist of the zero codeword, which is excluded from A. □

Lemma 7. *No $m + 1$ consecutive entries of any row of A can all be* 1.

Proof. If they were the cyclic set of codewords generated by the parity check polynomial would consist of the all ones codeword, which is excluded from A. □

Denote the minimum Hamming distance between any pair of codewords of the cyclic code by $d_{\min}$. It will be required that the initial cyclic code satisfies $d_{\min} > 4m + 4$.

Lemma 4 still holds with the appeals to Lemmas 1 and 2 in its proof replaced by appeals to Lemmas 6 and 7, respectively. As a consequence, Proposition 1 requires only slight modification to ensure that the block and the comb do not span more than half the length of the code:

Proposition 3. *If $2m^2 + 2m + 3 \leqslant (n-1)/2$, a set of positions $i_1, i_2, \ldots, i_{m+1}$ can be chosen so that*

(1) $i_1 = 2m + 1$ *and* $x_{i_1} = 1$,
(2) $i_1 \leqslant i_2 \leqslant \cdots \leqslant i_{m+1}$,
(3) $m + 1 \leqslant i_{j+1} - i_j \leqslant 2m$ *for* $1 \leqslant j \leqslant m - 1$,
(4) $m + 1 \leqslant i_{j+1} - i_j \leqslant 2m + 1$ *for* $j = m$,
(5) $i_{m+1} \leqslant (n-1)/2$

in such a way that no row of A is zero in all of these positions and no row of A is 1 *in all of these positions.*

With operation P defined as in Definition 1, Proposition 2 becomes:

Theorem 3. *Let A be the matrix corresponding to a cyclic code with $2m^2 + 2m + 3 \leqslant (n-1)/2$ and $d_{\min} > 4m + 4$. If the operation P is applied to A precisely once to give a new matrix $\tilde{A}$, then the rows of $\tilde{A}$ form a cyclically permutable code.*

Proof. An appeal to Lemma 5 similar to that in the proof of Proposition 2 shows that the Hamming distance between $P(S_i(\mathbf{x}^{(r)}))$ and $S_j(P(S_k(\mathbf{x}^{(v)})))$ is at least $d_{\min} - 4(m+1)$ ($i \not\equiv j + k \bmod n$) which is greater than 0. Thus it is only necessary to consider $i \equiv j + k \bmod n$. The remainder of the proof is identical to the proof of Proposition 2. □

Example 1. Let C be the dual of a *BCH* code of length $2^\gamma - 1$ and designed distance t. Then by the Carlitz–Uchiyama bound [4] both the inequalities in Theorem 3 are satisfied provided $\gamma \geqslant 11$ for $t = 2$, $\gamma \geqslant 13$ for $t = 3$, $\gamma \geqslant 14$ for $t = 4$, $\gamma \geqslant 15$ for $t = 5$. Thus the non-zero codewords of C are equivalent to a cyclically permutable code.

5. Conclusion

In this paper the question of whether certain cyclically permutable representations of codes exist has been answered constructively, and an application given. In general, long cyclic codes with large minimum distance relative to their dimension will always be equivalent (in the way described) to a cyclically permutable code.

References

[1] S. Bitan, T. Etzion, Constructions for optimal binary constant-weight cyclically permutable codes and difference families, IEEE Trans. Inform. Theory 41 (1995) 77–87.
[2] E.N. Gilbert, Cyclically permutable error-correcting codes, IEEE Trans. Inform. Theory 9 (1963) 175–182.
[3] X.D. Lin, K.H. Chang, Optimal PN sequence design for quasisynchronous CDMA communication systems, IEEE Trans. Comm. 45 (2) (1997) 221–226.
[4] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, ninth ed., Elsevier, Amsterdam, 1996.
[5] O. Moreno, Z. Zhang, P.V. Kumar, V.A. Zinoviev, New constructions of optimal cyclically permutable constant weight codes, IEEE Trans. Inform. Theory 41 (1995) 448–455.
[6] P.G. Neumann, On a class of cyclically permutable error-correcting codes, IEEE Trans. Inform. Theory IT-10 (1964) 75–78.
[7] N.Q.A.L. Györfi, J.L. Massey, Constructions of binary constant-weight cyclic codes and cyclically permutable codes, IEEE Trans. Inform. Theory 38 (1992) 940–949.
[8] W.W. Peterson, E.J. Weldon Jr., Error-Correcting Codes, second ed., MIT Press, Cambridge, MA, 1972.
[9] S. Sanusi, R.A. Jones, S. Perkins, D.H. Smith, The application of frequency assignment techniques in spreading code assignment, submitted for publication.
[10] S. Sriram, S. Hosur, Cyclically permutable codes for rapid acquisition in DS-CDMA systems with asynchronous base stations, IEEE J. Select. Areas in Comm. 19 (1) (2001) 83–94.